PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-224047
(43)Date of publication of application : 03.10.1991

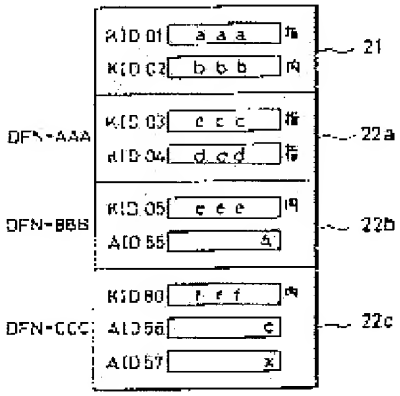
(51)Int.Cl. G06F 12/14
G06K 19/073

(21)Application number : 02-017924
(22)Date of filing : 30.01.1990

(71)Applicant : TOSHIBA CORP
(72)Inventor : IIJIMA YASUO

(54) PORTABLE ELECTRONIC DEVICE

(57)Abstract:
PURPOSE: To decide the propriety of accesses to a memory while keeping the security by deciding whether the key data used for confirmation belongs to a common data file or an application data file and then clearing the result of confirmation at selection of applications if the key data belongs to the application data file.
CONSTITUTION: A data memory consists of a common data file 21 which is used in common by all application and plural application data files 22a – 22c which are used individually by each application. Then it is decided whether they key data used for confirmation belongs to the common data file or the application data file. If the key data belongs to the latter data file, the result of confirmation of the application data file is cleared at selection of applications. Thus it is possible to decide the propriety of accesses to the data memory based on the result of confirmation while keeping the security among applications.



⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　平3－224047

⑤Int. Cl.[5]	識別記号	庁内整理番号	㊸公開　平成3年(1991)10月3日
G 06 F 12/14	320 C	7737－5B	
G 06 K 19/073		6711－5B　G 06 K 19/00　P	

審査請求　未請求　請求項の数 1　（全8頁）

㊹発明の名称　携帯可能電子装置

㉑特　願　平2－17924
㉒出　願　平2(1990)1月30日

㉒発明者　飯島　康雄　神奈川県川崎市幸区柳町70番地　株式会社東芝柳町工場内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉔代理人　弁理士　鈴江　武彦　外3名

明　細　書

1．発明の名称

携帯可能電子装置

2．特許請求の範囲

少なくともメモリと、このメモリに対してアクセスを行なう制御素子を有し、選択的に外部とのデータの授受を行なうもので、かつ前記メモリは、全てのアプリケーションで共通にアクセス対象となる第1の領域と、各アプリケーション個々に使用される少なくとも1つの第2の領域とに分割されているとともに、これら第1および第2の領域内に少なくとも1つのキーデータを有する携帯可能電子装置であって、

本装置の起動後は前記第1の領域のみアクセス対象とする手段と、

外部より前記第2の領域のうち1つを選択する選択情報を受信する第1の受信手段と、

この第1の受信手段により受信した選択情報に基づいて対応する第2の領域を選択的にアクセス可能とならしめる手段と、

少なくとも第1のデータを第1のキーデータにより暗号化された第1の暗号データを受信する第2の受信手段と、

第1のデータを選択された第2の領域に対応する第1のキーデータにより暗号化して第2の暗号データを生成する暗号化手段と、

この暗号化手段により生成した第2の暗号データと前記第2の受信手段により受信した第1の暗号データとを比較する比較手段と、

この比較手段の比較結果に基づいて前記メモリに対するアクセスの可否を判定する手段と、

新たに第2の領域のうち1つが選択されたときに前記比較結果の基となる第1のキーデータが前記第1の領域内に存在するか第2の領域内に存在するかを判断する手段と、

この判断の結果、第2の領域内に存在すると判断されると、前記比較結果の肯定結果を否定結果とする手段と

を具備したことを特徴とする携帯可能電子装置。

3．発明の詳細な説明

［発明の目的］

（産業上の利用分野）

本発明は、たとえば消去可能な不揮発性メモリおよびＣＰＵなどの制御素子を有するＩＣ（集積回路）チップを内蔵した、いわゆるＩＣカードと称される携帯可能電子装置に関する。

（従来の技術）

最近のＩＣカードに要求される機能として、外部装置（ＩＣカードを取扱う端末装置など）との相互認証機能が提案されている。この場合、外部装置との間で必ず相互認証を行なわなければ、アクセスが不可というようなアクセス制御方式がある。

（発明が解決しようとする課題）

この場合、ＩＣカードが多目的用途になるにつれ、アプリケーションごとに認証用のキーデータを有することが考えられるが、このとき例えばアプリケーションＡにおいて認証処理を施した結果がアプリケーションＢを運用する際にも使用可能であると、アプリケーション間のセキュリティ分離が困難である。

そこで、本発明は、各アプリケーションごとに異なる認証用のキーデータを有し、かつアプリケーション間のセキュリティを保ちつつ、認証結果によりメモリに対するアクセスの可否を決定することが可能な携帯可能電子装置を提供することを目的とする。

［発明の構成］

（課題を解決するための手段）

本発明は、少なくともメモリと、このメモリに対してアクセスを行なう制御素子を有し、選択的に外部とのデータの授受を行なうもので、かつ前記メモリは、全てのアプリケーションで共通にアクセス対象となる第１の領域と、各アプリケーション個々に使用される少なくとも１つの第２の領域とに分割されているとともに、これら第１および第２の領域内に少なくとも１つのキーデータを有する携帯可能電子装置であって、本装置の起動後は前記第１の領域のみアクセス対象とする手段と、外部より前記第２の領域のうち１つを選択する選択情報を受信する第１の受信手段と、この第１の受信手段により受信した選択情報に基づいて対応する第２の領域を選択的にアクセス可能とならしめる手段と、少なくとも第１のデータを第１のキーデータにより暗号化された第１の暗号データを受信する第２の受信手段と、第１のデータを選択された第２の領域に対応する第１のキーデータにより暗号化して第２の暗号データを生成する暗号化手段と、この暗号化手段により生成した第２の暗号データと前記第２の受信手段により受信した第１の暗号データとを比較する比較手段と、この比較手段の比較結果に基づいて前記メモリに対するアクセスの可否を判定する手段と、新たに第２の領域のうち１つが選択されたときに前記比較結果の基となる第１のキーデータが前記第１の領域内に存在するか第２の領域内に存在するかを判断する手段と、この判断の結果、第２の領域内に存在すると判断されると、前記比較結果の肯定結果を否定結果とする手段とを具備している。

（作用）

認証に使用したキーデータがコモンデータファイル（第１の領域）のものか、アプリケーションデータファイル（第２の領域）のものかを判断し、もしアプリケーションデータファイルのものであれば、アプリケーション選択時に認証結果をクリアするものである。これにより、各アプリケーションごとに異なるキーデータを持たせ、このキーデータで認証を行ない、その結果によりメモリに対するアクセスの可否を決定することによって成立するセキュリティ確保がアプリケーション間のセキュリティを保ちつつ行なえる。

（実施例）

以下、本発明の一実施例について図面を参照して説明する。

第６図は本発明に係る携帯可能電子装置としてのＩＣカードを取扱う端末装置の構成例を示すものである。すなわち、この端末装置８は、ＩＣカード１をカードリーダ・ライタ２を介してＣＰＵなどからなる制御部３と接続可能にするとともに、

制御部３にキーボード４、ＣＲＴディスプレイ装置５、プリンタ６およびフロッピィディスク装置７を接続して構成される。

ＩＣカード１は、ユーザが保持し、たとえば商品購入などの際にユーザのみが知得している暗証番号の参照や必要データの蓄積などを行なうもので、第５図にその機能ブロックを示すように、リード・ライト部１１、暗証設定・暗証照合部１２、および暗号化・復号化部１３などの基本機能を実行する部分と、これらの基本機能を管理するスーパバイザ１４とで構成されている。リード・ライト部１１は、後述するデータメモリ１６に対してデータの読出し、書込み、あるいは消去を行なう機能である。暗証設定・暗証照合部１２は、ユーザが設定した暗証番号の記憶および読出禁止処理を行なうとともに、暗証番号の設定後にその暗証番号の照合を行ない、以後の処理の許可を与える機能である。暗号化・復号化部１３は、たとえば通信回線を介して制御部３から他の端末装置へデータを送信する場合の通信データの漏洩、偽造を防止するための暗号化や暗号化されたデータの復号化を行なうものである。スーパバイザ１４は、カードリーダ・ライタ２から入力された機能コードもしくはデータの付加された機能コードを解読し、前記基本機能のうち必要な機能を選択して実行させる機能である。

これらの諸機能を発揮させるために、ＩＣカード１は例えば第４図に示すように、制御素子（たとえばＣＰＵ）１５、データメモリ１６、プログラムメモリ１７、およびカードリーダ・ライタ２との電気的接触を得るためのコンタクト部１８によって構成されており、これらのうち破線内の部分（制御素子１５、データメモリ１６、プログラムメモリ１７）は１つのＩＣチップ（あるいは複数のＩＣチップ）で構成されてＩＣカード本体内に埋設されている。

プログラムメモリ１７は、たとえばマスクＲＯＭで構成されており、前記各基本機能を実現するサブルーチンを備えた制御素子１５の制御プログラムなどを記憶するものである。

データメモリ１６は、各種データの記憶に使用され、たとえばＥＥＰＲＯＭなどの消去可能な不揮発性メモリで構成されている。

データメモリ１６は、たとえば第３図に示すように、全てのアプリケーションで共通に運用する１つのコモンデータファイル（以降、ＣＤＦと略称する）２１と、各アプリケーション個別に運用する複数のアプリケーションデータファイル（以降、ＡＤＦと略称する）２２ａ，２２ｂ，２２ｃとによって構成されており、各ＡＤＦ２２ａ，２２ｂ，２２ｃには、それぞれデータファイル名（ＤＦＮ）が付与されている。

そして、第３図の例においては、ＣＤＦ２１内には、キーデータ番号ＫＩＤ０１で示される指定用キーデータａａａ、およびキーデータ番号ＫＩＤ０２で示される内部キーデータｂｂｂが含まれ、またＤＦＮ－ＡＡＡで示されるＡＤＦ２２ａには、キーデータ番号ＫＩＤ０３で示される指定用キーデータｃｃｃ、およびキーデータ番号ＫＩＤ０４で示される指定用キーデータｄｄｄが含まれる。ＤＦＮ－ＢＢＢで示されるＡＤＦ２２ｂには、キーデータ番号ＫＩＤ０５で示される内部キーデータｅｅｅ、およびエリア番号ＡＩＤ５５で示されるデータエリアが含まれており、特にデータエリアはＡＤＦ２２ｂ内の内部キーデータによる認証処理で認証が確認されるとアクセス可能という属性情報（Ａ）が付与されている。また、ＤＦＮ－ＣＣＣで示されるＡＤＦ２２ｃには、キーデータ番号ＫＩＤ８０で示される内部キーデータｆｆｆ、エリア番号ＡＩＤ５６で示されるデータエリア、およびエリア番号ＡＩＤ５７で示されるデータエリアが含まれている。特に、エリア番号ＡＩＤ５６で示されるデータエリアは、ＣＤＦ２１内の内部キーデータによる認証処理で認証が確認されるとアクセス可能という属性情報（Ｃ）が付与されており、エリア番号ＡＩＤ５７で示されるデータエリアは、ＣＤＦ２１内の内部キーデータまたはＡＤＦ２２ｃ内の内部キーデータによる認証処理で認証が確認されるとアクセス可能という属性情報（Ｘ）が付与さ

れている。

ここに、指定用キーデータとは、端末装置８がＩＣカード１を認証するためのキーデータであり、内部キーデータとは、ＩＣカード１が端末装置８を認証するためのキーデータである。

次に、第１図を用いてＩＣカード１の動作概要を説明する。ＩＣカード１は、端末装置８から第２図（ａ）の電文を受信すると、その機能コードから選択的に第１図（ａ）の相互認証準備フローを実行する。これらの処理は、制御素子１５によりプログラムメモリ１７内のプログラムにしたがって行われる。すなわち、まずＡＤＦが選択済か否かを、内部ＲＡＭ（制御素子１５内のＲＡＭ）中の選択ＡＤＦ固有情報を参照することにより確認する。このとき、選択済でなければ、データメモリ１６上のＣＤＦ２１より、入力電文中のキーデータ番号（ＫＩＤ）を見つけ、また、選択済であれば、ＣＤＦ２１内とさらに選択済ＡＤＦ内よりＫＩＤを見つける。もし、この時点で見付からなければエラーステータスを出力する。なお、通常は起動時にはＣＤＦ２１が自動的に選択されている。

キーデータ番号（ＫＩＤ）を見つければ、対応するキーデータを内部的にリードし、正常か否かをチェックする。このとき、正常でなければエラーステータスを出力する。正常であれば、電文中の乱数情報Ａと該キーデータを内部ＲＡＭの所定領域に記憶しておく。次に、この乱数情報Ａと、カード発行時にセットされるカード固有の番号、それと、データメモリ１６内にあらかじめ初期値として記憶されているカード乱数情報とにより所定のアルゴリズムに従って乱数情報Ｂを生成し、これを新たなカード乱数情報として書き換えておく。

次に、再度ＡＤＦが選択済か否かを確認し、選択済でなければ、ＣＤＦ２１より内部キーデータのＫＩＤを見つけ、選択済であれば、ＣＤＦ２１内と更に選択済ＡＤＦ内よりＫＩＤをみつける（ＡＤＦが優先的に対象となる）。もし見つからなければ、エラーステータスを出力する。見つかったなら、対応するキーデータを内部的にリードし、正常か否かをチェックする。このとき、正常でなければエラーステータスを出力する。

さて、正常であれば、先に生成した乱数情報Ｂを、見つけた内部キーデータを暗号キーとして暗号化し、その結果を認証情報Ｃ２Ｘとして内部ＲＡＭの所定領域に記憶しておく。そして、内部キーデータのＫＩＤと乱数情報Ｂを出力し、本フローを終了する。

このフローにより、端末装置８とＩＣカード１との間の相互認証における乱数情報と、キー指定情報を共有することができる。

次に、第２図（ｂ）の電文を受信すると、その機能コードから選択的に第１図（ｂ）のフローを実行する。すなわち、まず先に説明した相互認証準備コマンドが実行済であるか否かを確認して、否であればエラーステータスを出力する。

実行済であれば、次に入力された電文中の認証情報Ｃ２と、先に内部ＲＡＭ上に記憶しておいた認証情報Ｃ２Ｘとを比較し、一致していれば一致フラグをオンし、そうでなければオフにする。このとき、一致フラグは、ＡＤＦの認証結果を示すＡＤＦ対応一致フラグと、ＣＤＦの認証結果を示すＣＤＦ対応一致フラグとがあり、内部キーデータが属するものがＡＤＦかＣＤＦかにより、ＡＤＦ対応一致フラグかＣＤＦ対応一致フラグかをオン，オフする。次に、先に内部ＲＡＭ上に記憶しておいた乱数情報Ａを、指定用キーデータを暗号キーとして暗号化し、その結果を認証情報Ｃ１Ｘとして先の一致フラグの結果と共に出力し、本フローを終了する。

このフローにより、端末装置８との相互認証が可能となる。

次に、第２図（ｃ）の電文を受信すると、その機能コードから選択的に第１図（ｃ）のＡＤＦ選択フローを実行する。すなわち、まず電文中のＤＦＮがＩＣカード１のデータメモリ１６に登録されているか否かを確認し、見つからなければエラーステータスを出力する。

もし見つければ、先のＣ２／Ｃ２Ｘの一致フ

グのうち、ＡＤＦ対応一致フラグをオフする。次に、指定ＤＦＮに対応する固有情報を内部ＲＡＭに保持し、正常終了ステータスを出力する。

次に、第２図（ｄ）で示すリードコマンド電文または第２図（ｅ）で示すライトコマンド電文を受信すると、その機能コードから選択的に第１図（ｄ）のフローを実行する。すなわち、まずＡＤＦが選択済か否かを判断し、選択済でなければ、ＣＤＦ２１内より入力電文中のエリア番号（ＡＩＤ）を見つけ、選択済であれば、選択済ＡＤＦ内とＣＤＦ２１内よりＡＩＤを見つける。このとき、見つからなければ、エラーステータスを出力する。　見つかれば、対応して記憶されているエリアの属性情報を参照し、先の一致フラグを確認する必要があるか否かを判断する。もし、必要であれば、それがＡＤＦ対応一致フラグかＣＤＦ対応一致フラグか、または、そのどちらでも良いかを判断する。

もし、ＡＤＦ対応一致フラグが必要、もしくはどちらでも良いという場合であれば、ＡＤＦ対応一致フラグを参照し、オンとなっているか否かをチェックする。もしオフであればエラーステータスを出力する。

また、ＣＤＦ対応一致フラグが必要、もしくはどちらでも良いという場合であれば、ＣＤＦ対応一致フラグを参照し、オンとなっているか否かをチェックする。もしオフとなっていればエラーステータスを出力する。

そして、電文中の機能コードにより、対応するリードまたはライト処理を施し、その処理結果を出力する。

次に、たとえば第３図のようなキーデータおよびエリアの構成に対するＩＣカード１の動作を説明する。第３図においては前述した通りであり、この状態で、ＡＤＦ選択を行なわない場合の相互認証には、指定用キーデータにはＫＩＤ０１のキーデータが使用され、内部キーデータにはＫＩＤ０２のキーデータが使用される。

また、ＤＦＮ－ＡＡＡによりＡＤＦ２２ａが選択された状態では、指定用キーデータにはＫＩＤ０３またはＫＩＤ０４のキーデータ、またはＫＩＤ０１のキーデータが使用され、内部キーデータとしてＫＩＤ０２のキーデータが使用される。

同様に、ＤＦＮ－ＢＢＢによりＡＤＦ２２ｂが選択された状態では、指定用キーデータにはＫＩＤ０１のキーデータが使用され、内部キーデータにはＫＩＤ０５のキーデータが使用される。

さて、ＡＤＦ２２ｂ内のＡＩＤ５５のエリアに対してアクセスするためには、このエリアの属性はＡＤＦ２２ｂ内の内部キーデータを必要とするようになっている。よって、ＡＤＦ２２ｂを選択した後の相互認証を行わなければならない。仮に、相互認証後にＡＤＦ２２ｂを選択すると、この相互認証に使用する内部キーデータはＫＩＤ０２のキーデータとなるからである。

また、ＡＤＦ２２ｃ内のＡＩＤ５６のエリアに対してのアクセスには、このエリアの属性がＣＤＦ２１内の内部キーデータを必要とするようになっている。よって、ＣＤＦ内部のキーデータＫＩＤ０２を用いた相互認証後にＡＤＦ２２ｃを選択し、エリアにアクセスしなければならない。したがって、ＣＤＦ対応一致フラグがオンになっていればアクセス可能である。

また、ＡＩＤ５７のエリアについては、内部キーデータを必要としていないので、ＣＤＦ２１内のキーデータＫＩＤ０２を用いた相互認証後にＡＤＦ２２ｃを選択しても、その逆、つまりＡＤＦ２２ｃを選択した後にＡＤＦ２２ｃ内のキーデータＫＩＤ０８によって相互認証を行なった後でもアクセス可能とならしめることになる。

したがって、特に最初にＡＤＦ２２ｂを選択し、相互認証を実行した後、次にＡＤＦ２２ｃを選択した場合、ＡＩＤ５７のエリアに対してアクセスはできない状態となる。

このように、認証に使用したキーデータがコモンデータファイル（ＣＤＦ）のものか、アプリケーションデータファイル（ＡＤＦ）のものかを判断し、もしアプリケーションデータファイルのものであれば、アプリケーション選択時にアプリケーションデータファイルの認証結果をクリアする

ものである。これにより、各アプリケーションごとに異なるキーデータを持たせ、このキーデータで認証を行ない、その結果によりデータメモリに対するアクセスの可否を決定することによって成立するセキュリティ確保がアプリケーション間のセキュリティを保ちつつ行なえる。

［発明の効果］

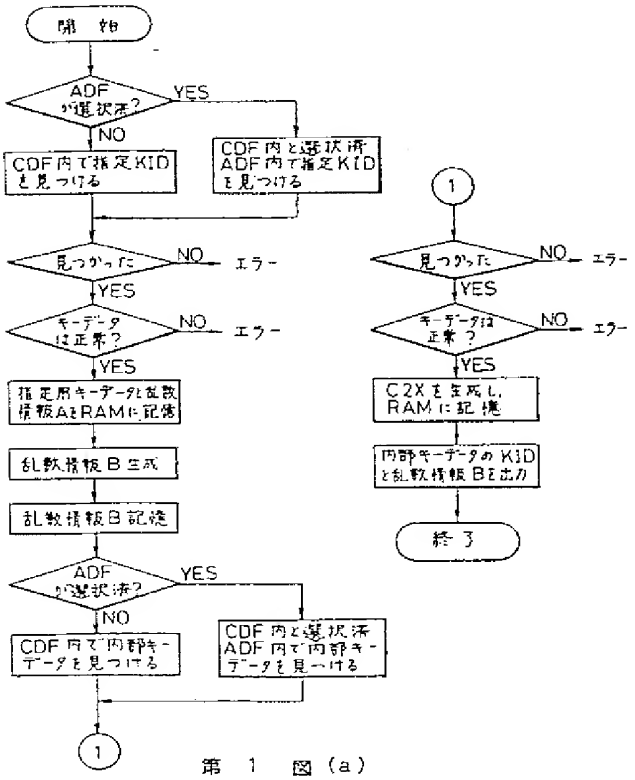
以上詳述したように本発明によれば、各アプリケーションごとに異なる認証用のキーデータを有し、かつアプリケーション間のセキュリティを保ちつつ、認証結果によりメモリに対するアクセスの可否を決定することが可能な携帯可能電子装置を提供できる。

4．図面の簡単な説明

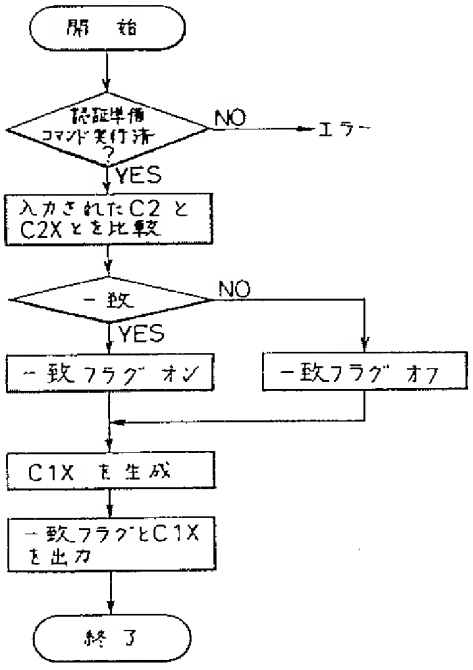
図は本発明の一実施例を説明するためのもので、第1図はICカードの動作概要を説明するフローチャート、第2図はICカードに入力される各種コマンド電文フォーマット例を示す図、第3図はデータメモリのファイル構造を示す図、第4図はICカードの概略構成を示すブロック図、第5図はICカードの機能ブロックを示す図、第6図は端末装置の構成を示すブロック図である。

1……ICカード（携帯可能電子装置）、8……端末装置、15……制御素子、16……データメモリ（不揮発性メモリ）、17……プログラムメモリ、21……コモンデータファイル（CDF、第1の領域）、22a，22b，22c……アプリケーションデータファイル（ADF、第2の領域）。

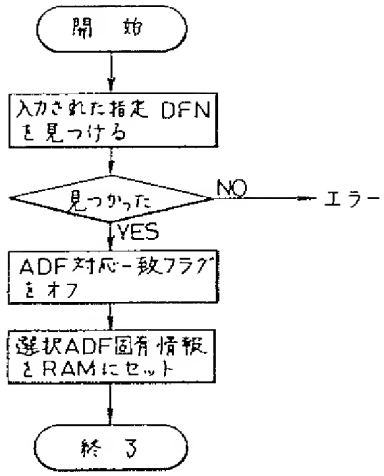
出願人代理人　弁理士　鈴江武彦



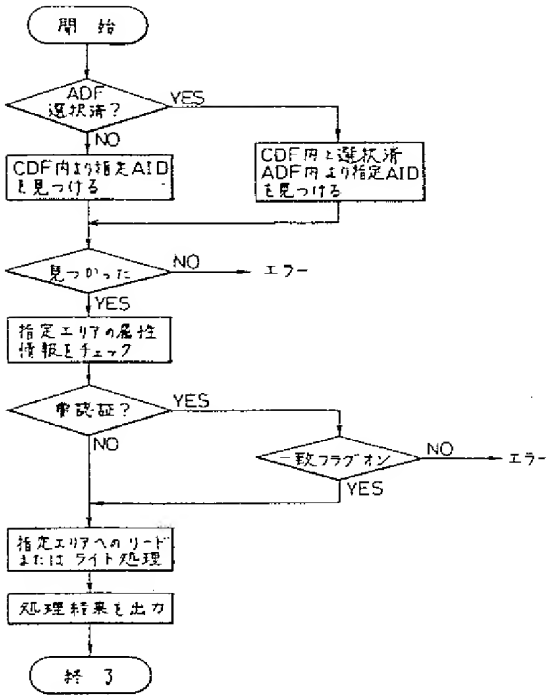
第　1　図（a）



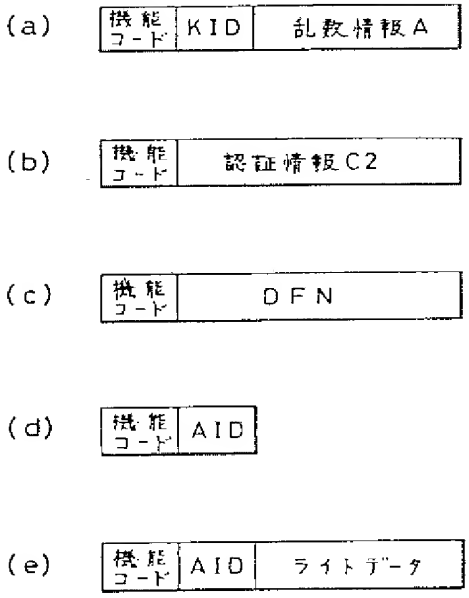
第　1　図（b）



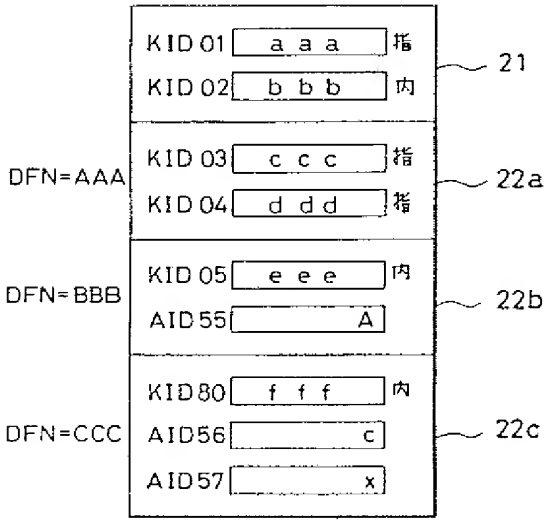
第 1 図（c）



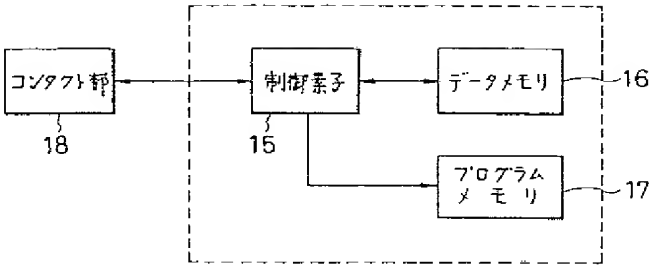
第 1 図（d）



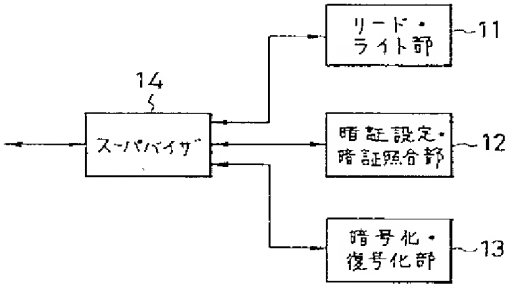
第 2 図



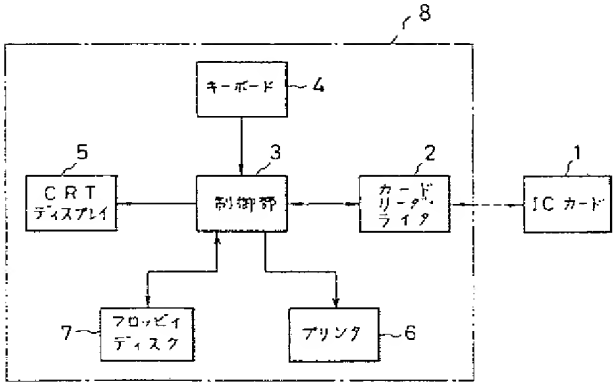
第 3 図


コンタクト部
18
制御素子
15
データメモリ
16
プログラム
メモリ
17

第 4 図


14
スーパバイザ
リード・
ライト部
11
暗証設定・
暗証照合部
12
暗号化・
復号化部
13

第 5 図


8
キーボード
4
5
CRT
ディスプレイ
3
制御部
2
カード
リーダ・
ライタ
1
IC カード
7
フロッピィ
ディスク
プリンタ
6

第 6 図